Chapter 3 System Management

This chapter discusses the various tools and utilities that allow for the system management of the HP Workstation xw4200. This chapter includes the following sections:

Computer Setup (F10)

The Computer Setup (F10) utilities enable you to perform the following tasks:

- Change factory default settings and to set or change the system configuration, which might be necessary when you add or remove hardware.
- Determine if all of the devices installed on the workstation are recognized by the system and functioning properly.
- Determine information about the operating environment of the workstation.
- Solve system configuration errors detected but not automatically fixed during the Power-On Self-Test (POST).
- Establish and manage passwords and other security features.
- Establish and manage energy-saving timeouts (not supported for Linux platforms).
- Modify or restore factory default settings.
- Set the system date and time.
- Set, view, change, or verify the system configuration including settings for processor, graphics, memory, audio, storage, communications, and input devices.
- Modify the boot order of bootable devices, such as hard drives, diskette drives, optical drives, or LS-120 drives.
- Configure the boot priority of SATA, IDE (ATA) and SCSI hard drive controllers.
- Enable Quick Boot which is faster than Full Boot, but does not run all of the diagnostic tests run during a Full Boot. You can set your system to:
  - always Quick Boot (default)
  - periodically Full Boot (from every 1–30 days)
  - always Full Boot
- Enable or disable Network Server Mode, which allows the workstation to boot the operating system when the power-on password is enabled with or without a keyboard or mouse attached. When attached to the system, the keyboard and mouse remain locked until the power-on password is entered.
- Select POST Messages Enabled or Disabled to change the display status of POST messages. POST Messages Disabled suppresses most POST messages, such as memory count, product name, and other non-error text messages. If a POST error occurs, the error is displayed regardless of the mode selected. To manually switch to POST Messages Enabled during POST, press any key (except **F1** through **F12**).
- Establish an Ownership Tag, the text of which is displayed each time the system is turned on or restarted.
- Enter the Asset Tag or property identification number assigned by your company to this workstation.
- Enable power-on password prompting during system restarts (warm boots) as well as during power-on.
- Secure the integrated I/O functionality, including the serial, USB, or parallel ports, audio, or embedded NIC, so that they cannot be used until they are unsecured.
- Enable or disable Master Boot Record (MBR) Security.

- Enable or disable removable media boot ability.
- Enable or disable removable media write ability (when supported by hardware).
- Replicate your system setup by saving system configuration information on diskette and restoring it on one or more workstations.
- Execute self-tests on a specified SATA or IDE (ATA) hard drive (when supported by the drive).

NOTE All features identified in this chapter might not be available on all HP products.

BIOS ROM

The Basic Input/Output System (BIOS) of the workstation is a collection of machine language programs stored as firmware in read-only memory (ROM). The BIOS ROM includes such functions as POST, PCI device initialization, Plug 'n Play support, power management activities, and the Setup utility. The firmware contained in the BIOS ROM supports the following systems and specifications:

- Microsoft WHQL
- Alert-On-LAN (AOL) and Wake-On-LAN (WOL)
- ACPI 1.0 and OnNow
- SMBIOS 2.3.5
- PC98/99/00 and NetPC
- PXE boot ROM for the integrated LAN controller
- BIOS Boot Specification 1.01
- Enhanced Disk Drive Specification 3.0
- “El Torito” Bootable CD-ROM Format Specification 1.0
- ATAPI Removable Media Device BIOS Specification 1.0
- MPS Specification 1.4 (for booting Linux SMP)

The BIOS ROM is a 512-KB Firmware Hub (or Firmware Hub-compatible) part. The runtime portion of the BIOS resides in a 128-K block from E0000h to FFFFFh.

Using Computer Setup (F10)

Computer Setup can be accessed only by turning on the workstation or restarting the system. To access the Computer Setup Utilities menu:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart the Computer**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must try again. Turn the workstation off, then on again, and press the **F10** key again to access the utility.

3. Select your language from the list and press **Enter**. A choice of four headings appears in the Computer Setup Utilities menu: File, Storage, Security, and Advanced.
4. Use the arrow (left and right) keys to select the appropriate heading. Use the arrow (up and down) keys to select the option you want, then press **Enter**.
5. To apply and save changes, select **File>Save Changes and Exit**.
   - If you have made changes that you do not want applied, select **Ignore Changes and Exit**.
   - To reset to factory settings, select **Set Defaults and Exit**. This option will restore the original factory system defaults.

CAUTION Do NOT turn the workstation power OFF while the ROM is saving your Computer Setup F10 changes because the CMOS could become corrupted. It is safe to turn off all power to the workstation after you exit the F10 Setup screen.

NOTE This menu can change with new firmware releases, so it might be consistent with what is presented in the following table.

Table 3-1 Computer Setup Menu

Heading	Option	Description
File	System Information	Lists product name, processor type/speed/stepping, cache size (L1/L2), system ROM family and version, installed memory size, chassis serial number, integrated MAC for enabled or embedded NIC (if applicable), and asset tracking number.
	About	Displays copyright information.
	Set Time and Date	Allows you to set system time and date.
	Replicated Setup	**Save to Removable Media** Saves system configuration, including CMOS, to a formatted blank 1.44-MB diskette in file CPQsetup.txt.
		Restore to Removable Media Restores system configuration from a diskette.
	Default Setup	**Save Current Settings as Default** Saves the current settings as default settings for the next operation.
		Restore Factory Settings as Default Restores the factory settings as the default settings for the next operation.
	Apply Defaults and Exit	Restores factory default settings which includes clearing any established passwords.
	Ignore Changes and Exit	Exits Computer Setup without applying or saving any changes.
	Save Changes and Exit	Saves changes to system configuration and exits Computer Setup.

Table 3-1 Computer Setup Menu (Continued)

Heading	Option	Description
Storage	Device Configuration	Lists all installed non-SCSI storage devices. SCSI storage drives will not be listed in Computer Setup (F10). When a device is selected, detailed information and options are displayed. The following options might be presented:
		Diskette Type *(for legacy diskette drives only)* Identifies the highest capacity media type accepted by the diskette drive. Options are 3.5" 1.44 MB, 5.25" 1.2 MB, and Not Installed.
		Drive Emulation *(IDE devices only)* Allows you to select a drive emulation type for a storage device. (For example, a Zip drive can be made bootable by selecting disk emulation.)
		Drive Type / **Emulation Options** ATAPI Zip drive: None (treated as Other). Diskette (treated as diskette drive). Disk (treated as hard drive). IDE Hard disk: None (treated as Other). Disk (treated as hard drive). Legacy diskette: No emulation options available. IDE CD-ROM: No emulation options available. ATAPI LS-120: No emulation options available.
		Transfer Mode *(IDE devices only)* Specifies the active data transfer mode. Options (subject to device capabilities) are PIO 0, Max PIO, Enhanced DMA, Ultra DMA 0, and Max UDMA.
		Translation Mode *(IDE disks only)* Lets you select the translation mode to be used for the device. This enables the BIOS to access disks partitioned and formatted on other systems and may be necessary for users of older versions of UNIX (for example, SCO UNIX version 3.2). Options are Bit-Shift, LBA Assisted, User, and None. **CAUTION:** A new Automatic option has been added to allow for BIOS to automatically determine the translation mode used to configure a previously formatted IDE, SATA, or USB mass storage device. This prevents you from having to know how the mass storage device was previously formatted. Ordinarily, the translation mode selected automatically by the BIOS should not be changed. If the selected translation mode is not compatible with the translation mode that was active when the disk was partitioned and formatted, the data on the disk will be inaccessible.
		Translation Parameters *(IDE disks only)* Allows you to specify the parameters (logical cylinders, heads, and sectors per track) used by the BIOS to translate disk I/O requests (from the operating system or an application) into terms the hard drive can accept. Logical cylinders cannot exceed 1024. The number of heads cannot exceed 256. The number of sectors per track cannot exceed 63. These fields are only visible and changeable when the drive translation mode is set to User.
		Multisector Transfers *(IDE disks only)* Specifies how many sectors are transferred per multi-sector PIO operation. Options (subject to device capabilities) are Disabled, 8, and 16.

Table 3-1 Computer Setup Menu (Continued)

Heading	Option	Description
Storage *(continued)*	Options	**Removable Media Boot** Enables/disables ability to boot the system from removable media.
		Legacy Diskette Write Enables/disables ability to write data to removable media. **NOTE:** This feature applies only to legacy diskette, (IDE/ATA) LS-120 Superdisk, (IDE/ATA) LS-240 Superdisk, and (IDE/ATA) PD-optical drives. **NOTE:** After saving changes to Removable Media Boot, the workstation will restart. Manually, turn the workstation off, then on.
		BIOS DMA Data Transfers Allows you to enable or disable the BIOS use of DMA for IDE data transfers.
		IDE Controller Allows you to enable or disable the primary IDE/ATA controller.
		SATA Emulation Enables the SATA to emulate the RAID controller, combined controllers, or a separate controller.
		SATA Primary Controller Allows you to disable the SATA primary controller ports.
		SATA Secondary Controller Allows you to disable the SATA secondary controller ports.
		Diskette MBR Validation Allows you to enable or disable strict validation of the diskette MBR. **NOTE:** If you use a bootable diskette image that you know to be valid, and it does not boot with Diskette MBR Validation enabled, you might need to disable this option to use the diskette.
	IDE DPS Self-Test	Allows you to execute self-tests on IDE hard drives capable of performing the Drive Protection System (DPS) self-tests. **NOTE:** This selection will only appear when at least one drive capable of performing the IDE DPS self-tests is attached to the system.
	Controller Order*	Allows you to specify the order of the attached hard drive controllers. The first hard drive controller in the order will have priority in the boot sequence and will be recognized as drive C (if any devices are attached). **NOTE:** The selection will not appear if all hard drives are attached to the embedded IDE controllers.
	Boot Order	Allows you to configure the boot, diskette drive, and hard drive orders by physically reordering the menu entries. Each device on the list can be individually excluded from or included for consideration as a bootable operating system source. **NOTE:** MS-DOS drive lettering assignments might not apply after a non-MS-DOS operating system has started. **Shortcut to Temporarily Override Boot Order** To boot **one time** from a device other than the default device specified in Boot Order, restart the workstation and press **F9** when the `F10=Setup` message appears on the screen. After POST is completed, a list of bootable devices is displayed. Use the arrow keys to select the preferred bootable device and press **Enter.** The workstation then boots from the selected non-default device for this one time.

*Available on select models.

Table 3-1 Computer Setup Menu (Continued)

Heading	Option	Description
Security	Setup Password	Allows you to set and enables setup (administrator) password. **NOTE:** If the setup password is set, it is required to change Computer Setup options, flash the ROM, and make changes to certain Plug 'n Play settings under Windows.
	Power-On Password	Allows you to set and enable power-on password.
	Device Security*	Enables/disables serial ports A and B, parallel port, front USB ports, all USB ports, system audio, network controllers (some models), and SCSI controllers (some models).
	Network Service Boot	Enables/disables the workstation's ability to boot from an operating system installed on a network server. (Feature available on NIC models only; the network controller must reside on the PCI bus or be embedded on the system board.)
	Password Options (This selection will appear only if a power-on password is set.)	Allows you to specify whether the password is required for warm boot (**CTRL+ALT+DEL**).
	Hood sensor*	Allows you to enable/disable solenoid hood (Smart Cover) lock. **NOTE:** *Notify User* alerts the user that the sensor has detected that the cover has been removed. *Setup Password* requires that the setup password be entered to boot the workstation if the sensor detects that the cover has been removed. This feature is supported on select models only.
	DriveLock*	Allows you to assign or modify a master or user password for certain hard drives. When enabled, the user is prompted to provide one of the DriveLock passwords during POST. If neither is successfully entered, the hard drive will remain inaccessible until one of the passwords is successfully provided during a subsequent cold-boot sequence. This selection will only appear when at least one drive that supports the DriveLock feature is attached to the system.
	Master Boot Record Security*	Allows you to enable or disable MBR Security. When enabled, the BIOS rejects all requests to write to the MBR on the current bootable disk. Each time the workstation is powered on or rebooted, the BIOS compares the MBR of the bootable disk to the previously saved MBR. If changes are detected, you are given the option of saving the MBR on the current bootable disk, restoring the previously saved MBR, or disabling MBR security. You must know the setup password if one is set. **NOTE:** Disable MBR Security before intentionally changing the formatting or partitioning of the current bootable disk. Several disk utilities (such as FDISK and FORMAT) attempt to update the MBR. If MBR Security is enabled and disk accesses are being serviced by the BIOS, write requests to the MBR are rejected, causing the utilities to report errors. If MBR Security is enabled and disk accesses are being serviced by the operating system, any MBR change will be detected by the BIOS during the next reboot, and an MBR Security warning message will be displayed.
	Save Master Boot Record*	Saves a backup copy of the Master Boot Record of the current bootable disk. **NOTE:** Only appears if MBR Security is enabled.
	System IDs	Allows you to set: - Asset tag (18-byte identifier) and ownership Tag (80-byte identifier displayed during POST). - Chassis serial number or Universal Unique Identifier (UUID) number. The UUID can only be updated if the current chassis serial number is invalid. (These ID numbers are normally set in the factory and are used to uniquely identify the system.) - Keyboard locale setting (for example, English or German) for System ID entry.

*Available on select models

Table 3-1 Computer Setup Menu (Continued)

Heading	Option	Description
Security *(continued)*	Restore Master Boot Record*	Restores the backup Master Boot Record to the current bootable disk. **NOTE:** Only appears if all of the following conditions are true: - MBR Security is enabled. - A backup copy of the MBR has been previously saved. - The current bootable disk is the same disk from which the backup copy of the MBR was saved. **NOTE:** Restoring a previously saved MBR after a disk utility or operating system has modified the MBR might cause the data on the disk to become inaccessible. Only restore a previously saved MBR if you are confident that the current bootable disk's MBR has been corrupted or infected with a virus.
	Smarter	Allows you to use Smarter authentication for the Pre-Boot process.
	Embedded Security Device	**Embedded Security Device** Allows you to activate the Trusted Platform Module. Setup password must be established before this menu item can be selected.
		Reset to Factory Settings Allows you to clear all encryption keys stored into the Trusted Platform Module. Setup password must be established before this menu item can be selected.
	Device Security	SMBUS Controller was added to embedded devices capable of being hidden or available during a refresh of the BIOS.
Power	OS Power Management	Allows you to enable PCI Express ASPM support.
	Thermal	Allows you set the fan idle mode.

*Available on select models.

Table 3-1 Computer Setup Menu (Continued)

Heading	Option	Description
Advanced**	Power-On Options	Allows you to set: - POST mode (QuickBoot, FullBoot, or FullBoot every 1–30 days). - POST messages (enable/disable). - Safe POST* (enable/disable). Enabling this feature allows the ROM to monitor add-in cards during boot. If an add-in card does not work or initialize correctly, then on the next boot all cards will be skipped during POST. - **F9** prompt (enable/disable). Enabling this feature will display the text `F9=Boot Menu` during POST. Disabling this feature prevents the text from being displayed but pressing **F9** will still access the Shortcut Boot (Order) Menu screen. Refer to **Storage>Boot Order** for more information. - **F10** prompt (enable/disable). Enabling this feature will display the text `F10=Setup` during POST. Disabling this feature prevents the text from being displayed but pressing **F10** will still access the Setup screen. - **F12** prompt (enable/disable). Enabling this feature will display the text `F12=Network Service Boot` during POST. Disabling this feature prevents the text from being displayed but pressing **F12** will still force the system to attempt booting from the network. - Option ROM* prompt (enable/disable). Enabling this feature will cause the system to display a message before loading options ROMs. - Remote wakeup boot source (remote server/local hard drive). - Fan Idle Mode: Allows you set the fan idle mode. - After Power Loss (off/on/previous state): After power loss, if you connect your workstation to an electric power strip and would like to turn on power to the workstation using the switch on the power strip, set this option to ON. The previous state will set the power loss setting to whatever the unit status was before the power loss. - If you turn off power to your workstation using the switch on a power strip, you will not be able to use the suspend/sleep feature or the Remote Management features. - POST Delay (in seconds) (enable/disable). Enabling this feature will add a user-specified delay to the POST process. This delay is sometimes needed for hard disks on some PCI cards that spin up very slowly; so slowly that they are not ready to boot by the time POST is finished. The POST delay also gives you more time to select **F10** to enter Computer Setup (F10). - I/O APIC Mode (enable/disable). Enabling this feature will allow Microsoft Windows Operating system to run optimally. This feature must be disabled for certain non-Microsoft Operating Systems to work properly. - ACPI/USB Buffers @ Top of Memory (enable/disable). Enabling this feature places USB memory buffers at the top of memory. The advantage of remapping is that it allows space in the DOS Compatibility Hole range, below 1-MB, to be made available for additional PCI plug-in cards that need option ROM space.
	BIOS Power-On	Allows you to select week days and a specific time to automatically power the unit on from the power-off state.
	Onboard Devices	Allows you to set resources for or disable onboard system devices (serial port, parallel port, or diskette controller).
	PCI Devices	Lists currently installed PCI devices and their IRQ settings. Allows you to reconfigure IRQ settings for these devices or to disable them entirely. These settings have no effect under an APIC-based operating system.
	Bus Options*	Allows you to enable or disable: - PCI bus mastering, which allows a PCI device to take control of the PCI bus. - PCI VGA palette snooping, which sets the VGA palette snooping bit in PCI configuration space; only needed when more than one graphics controller is installed. - PCI SERR# generation. - ECC support allows hardware-based error correction for ECC-capable memories.

*Available on select models.
**These options should be used by advanced users only.

Table 3-1 Computer Setup Menu (Continued)

Heading	Option	Description
Advanced** *(continued)*	Device options	Allows you to set: - Printer mode (bi-directional, EPP+ECP, output only). - Num Lock state at power-on (off/on). - Power management event (PME) wakeup events (enable/disable). - Processor cache (enable/disable). - Hyper-Threading* (enable/disable). - ACPI S3* support (enable/disable). S3 is an advanced configuration and power interface (ACPI) sleep state that some add-in hardware options might not support. - ACPI S3 selections are supported on select models only. If the ACPI S3 support option is not presented, the other ACPI S3 options (ACPI S3 Video REPOST, ACPI S3 Hard disk Reset, and ACPI S3 PS2 Mouse Wakeup) will not be available. - ACPI S3 Video REPOST* (enable/disable). This feature reruns the video option ROM on a boot from the S3 state. - ACPI S3 Hard Disk Reset* (enable/disable). Resets the hard disk on a boot from the S3 sleep state. - ACPI S3 PS2 Mouse Wakeup* (enable/disable). Allows the mouse to wake the system from the S3 sleep state. - Aperture size*. Allows you to specify the amount of system memory reserved for use by your graphics controller. - Monitor Tracking (enable/disable). Allows ROM to save monitor asset information. - Unique Sleep State Blink Patterns*. Allows you to choose a LED blink pattern that uniquely identifies each sleep state. - Frame Buffer Size*. Allows you to specify amount of system memory dedicated to the embedded graphics frame buffer. The AUTO setting attempts to optimize the frame buffer size depending on the amount of total system memory. - PCI Slot x Option ROM Download. Allows you to enable/disable the downloading of the PCI slot option ROM. “X.” can be a value of 1, 2, 3, 4, or 5. - NIC PXE (enable/disable). The BIOS contains an embedded NIC option ROM to allow the unit to boot through the network to a PXE server. This is typically used to download a corporate image to a hard drive. The NIC option ROM takes up memory space below 1-MB commonly referred to as DOS Compatibility Hole (DCH) space. This space is limited. The F10 option allows you to disable the downloading of the embedded NIC option ROM, giving more DCH space for other PCI cards which might need option ROM space. The default setting for the NIC option ROM is “enabled.”
	PCI VGA Configuration	Displayed only if there are multiple PCI video adapters in the system. Allows you to specify which VGA controller will be the “boot” or primary VGA controller.

*Available on select models.
**These options should be used by advanced users only.

Desktop Management

HP Client Management Solutions (available for download from http://www.hp.com/go/workstationsupport) provides standards-based solutions for managing and controlling workstations in a networked environment. This section summarizes the capabilities and features of the key components of desktop management:

- Initial Configuration and Deployment
- Remote System Installation
- Software Updating and Management
- ROM Flash
- Asset Tracking and Security
- Fault Notification and Recovery

NOTE Support for specific features described in this guide might vary by model or software version.

Initial Configuration and Deployment

The workstation comes with a preinstalled system software image. After a brief software “unbundling” process, the workstation is ready to use.

You may prefer to replace the preinstalled software image with a customized set of system and application software. There are several methods for deploying a customized software image. They include:

- Installing additional software applications after unbundling the preinstalled software image.
- Using software deployment tools, such as Altiris Deployment Solutions™, to replace the preinstalled software with a customized software image.
- Using a disk cloning process to copy the contents from one hard drive to another.

The best deployment method depends on your information technology environment and processes. The PC Deployment section of the HP Lifecycle Solutions Web site (http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html) provides information to help you select the best deployment method.

The Restore Plus! CD, ROM-based setup, and ACPI hardware provide further assistance with recovery of system software, configuration management and troubleshooting, and power management.

Remote System Installation

Remote System Installation lets you start and set up your system using the software and configuration information located on a network server. This feature is usually used as a system setup and configuration tool, and can be used for the following tasks:

- Deploying a software image on one or more new PCs
- Formatting a hard drive
- Installing application software or drivers
- Updating the operating system, application software, or drivers

To initiate Remote System Installation, press **F12** when the `F12=Network Service Boot` message appears in the lower-right corner of the HP logo screen. Follow the on-screen instructions to continue the process. The default boot order is a BIOS configuration setting that can be changed to always attempt to PXE boot.

HP and Altiris have partnered to provide tools designed to make the task of corporate PC deployment and management easier and less time-consuming, ultimately lowering the total cost of ownership and making HP PCs the most manageable client PCs in the enterprise environment.

Software Updating and Management

HP provides several tools for managing and updating software on desktops and workstations—HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification; and Subscriber's Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) assists HP customers in managing the hardware aspects of their client workstations with features that include:

- Detailed views of hardware inventory for asset management
- PC health check monitoring and diagnostics
- Proactive notification of changes in the hardware environment
- Web-accessible reporting of business critical details such as machines with thermal warnings, memory alerts, and more
- Remote updating of system software such as device drivers and ROM BIOS
- Remote changing of boot order
- Configuring the system BIOS settings

For more information on the HP Client Manager, visit http://www.hp.com/go/im.

Altiris Client Management Solutions

HP and Altiris have partnered to provide comprehensive, tightly integrated systems management solutions to reduce the cost of owning HP client PCs. HP Client Manager Software is the foundation for additional Altiris Client Management Solutions that address:

- Inventory and Asset Management
  - SW license compliance
  - PC tracking and reporting
  - Lease contract, fixing asset tracking
- Deployment and Migration
  - Microsoft Windows XP Professional or Home Edition migration
  - System deployment
  - Personality migrations

- Help Desk and Problem Resolution
  - Managing help desk tickets
  - Remote troubleshooting
  - Remote problem resolution
  - Client disaster recovery
- Software and Operations Management
  - Ongoing desktop management
  - HP system SW deployment
  - Application self-healing

For more information and details on how to download a fully-functional 30-day evaluation version of the Altiris solutions, visit http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

System Software Manager (SSM) is a utility that lets you update system-level software on multiple systems simultaneously. When executed on a PC client system, SSM detects both hardware and software versions, then updates the appropriate software from a central repository, also known as a file store. Driver versions that are supported by SSM are denoted with a special icon on the software, the driver download Web site, and on the Support Software CD. To download the utility or to obtain more information on SSM, visit http://www.hp.com/go/ssm.

Proactive Change Notification

The Proactive Change Notification program uses the Subscriber's Choice Web site in order to proactively and automatically:

- Send you Proactive Change Notification (PCN) e-mails informing you of hardware and software changes to most commercial workstations and servers, up to 60 days in advance.
- Send you e-mail containing Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins, and Driver alerts for most commercial workstations and servers.

You create your own profile to ensure that you only receive the information relevant to a specific IT environment. To learn more about the Proactive Change Notification program and create a custom profile, visit http://www.hp.com/go/pcn.

Subscriber’s Choice

Subscriber’s Choice is a client-based service from HP. Based on your profile, HP will supply you with personalized product tips, feature articles, and/or driver and support alerts/notifications. Subscriber’s Choice Driver and Support Alerts/Notifications will deliver e-mails notifying you that the information you subscribed to in your profile is available for review and retrieval. To learn more about Subscriber’s Choice and create a custom profile, visit http://www.hp.com/go/pcn.

ROM Flash

The workstation comes with a programmable flash ROM (read only memory). By establishing a setup password in the Computer Setup (F10) Utility, you can protect the ROM from being unintentionally updated or overwritten. This is important to ensure the operating integrity of the workstation. Should you need or want to upgrade the ROM, you may:

- Order an upgraded ROMPaq diskette from HP.
- Download the latest ROMPaq images from HP driver and support page, http://www.hp.com/support/ files.

CAUTION For maximum ROM protection, be sure to establish a setup password. The setup password prevents unauthorized ROM upgrades. System Software Manager allows the system administrator to set the setup password on one or more PCs simultaneously. For more information, visit http://www.hp.com/go/ssm.

Remote ROM Flash

Remote ROM Flash allows the system administrator to safely upgrade the ROM on remote HP workstations directly from the centralized network management console. Enabling the system administrator to perform this task remotely, on multiple workstations and personal computers, results in a consistent deployment of and greater control over HP PC ROM images over the network. It also results in greater productivity and lower total cost of ownership.

The workstation must be powered on, or turned on through Remote Wakeup, to take advantage of Remote ROM Flash.

For more information on Remote ROM Flash, refer to the HP Client Manager Software or System Software Manager at http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

The HPQFlash utility is used to locally update or restore the system ROM on individual PCs through a Windows operating system.

For more information on HPQFlash, visit http://www.hp.com/support/files and enter the name of the workstation when prompted.

FailSafe Boot Block ROM

The FailSafe Boot Block ROM allows for system recovery in the unlikely event of a ROM flash failure, for example, if a power failure were to occur during a ROM upgrade. The Boot Block is a flash-protected section of the ROM that checks for a valid system ROM flash when power to the system is turned on.

- If the system ROM is valid, the system starts normally.
- If the system ROM fails the validation check, the FailSafe Boot Block ROM provides enough support to start the system from a ROMPaq diskette, which will program the system ROM with a valid image.

NOTE Some models also support recovery from a ROMPaq CD. ISO ROMPaq images are included with selected models in the downloadable ROM softpaqs.

When the boot block detects an invalid system ROM, the System Power LED blinks RED 8 times, one every second, followed by a 2-second pause. Also, eight simultaneous beeps will be heard. A Boot Block recovery mode message is displayed on the screen (some models).

To recover the system after it enters Boot Block recovery mode:

1. If there is a diskette in the diskette drive or a CD in the CD drive, remove the diskette and CD and turn off the power.
2. Insert a ROMPaq diskette into the diskette drive or, if permitted on this workstation, a ROMPaq CD into the CD drive.
3. Turn on the workstation.

   If no ROMPaq diskette or ROMPaq CD is found, you will be prompted to insert one and restart the workstation.

   If a setup password has been established, the Caps Lock light will turn on and you will be prompted to enter the password.
4. Enter the setup password.

   If the system successfully starts from the diskette and successfully reprograms the ROM, then the three keyboard lights will turn on. A rising tone series of beeps also signals successful completion.
5. Remove the diskette or CD and turn the power off.
6. Turn the power on again to restart the workstation.

The following table lists the various keyboard light combinations used by the Boot Block ROM (when a PS/2 keyboard is attached to the workstation), and explains the meaning and action associated with each combination.

Table 3-2 Keyboard Light Combinations Used by Boot Block ROM

FailSafe Boot Block Mode	Keyboard LED Activity	State/Message
Num Lock	On	ROMPaq diskette or ROMPaq CD not present, is bad, or drive not ready.
Caps Lock	On	Enter password.
Num, Caps, Scroll Lock	Blink On in sequence, one at a time–N,C, SL	Keyboard locked in network mode.
Num, Caps, Scroll Lock	On	Boot Block ROM Flash successful. Turn power off, then on to reboot.

NOTE: Diagnostic lights do not flash on USB keyboards

Replicating the Setup

The following procedures give an administrator the ability to easily copy one setup configuration to other workstations of the same model. This allows for faster, more consistent configuration of multiple workstations.

NOTE Both procedures require a diskette drive.

NOTE To collect and replicate BIOS settings on multiple computers, use System Software Manager or HP Client Manager Software. For more information, visit http://www.hp.com/go/easydeploy.

COPYING TO SINGLE WORKSTATION

CAUTION A setup configuration is model-specific. File system corruption may result if source and target workstations are not the same model. For example, do not copy the setup configuration from an HP Workstation xw8200 to an HP Workstation xw4200.

1. Select a setup configuration to copy. Turn off the workstation. If you are in Windows, click **Start>Shut Down>Shut Down**.
2. Turn on the workstation.
3. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

4. If you are using a a diskette, insert it now.
5. Select **File>Replicated Setup>Save to Removable Media**. Follow the instructions on the screen to create the configuration diskette.
6. Turn off the workstation to be configured and insert the configuration diskette.This procedure gives an administrator the ability to easily copy one setup configuration to other workstations of the same model. This allows for faster, more consistent configuration of multiple workstations.
7. Turn on the workstation to be configured.
8. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.
9. Select **File>Replicated Setup>Restore from Removable Media**, and follow the instructions on the screen.
10. Restart the workstation when the configuration is complete.

COPYING TO MULTIPLE WORKSTATIONS

CAUTION A setup configuration is model-specific. File system corruption may result if source and target workstations are not the same model. For example, do not copy the setup configuration from a xw6200 to a xw4200.

This method takes a little longer to prepare the configuration diskette, but copying the configuration to target workstations is significantly faster.

NOTE A bootable diskette is required for this procedure. If Windows XP is not available to use to create a bootable diskette, use the method for copying to a single workstation instead (see "Copying to Single Workstation" on page 49).

1. Create a bootable diskette.
2. Select a setup configuration to copy. Turn off the workstation. If you are in Windows, click **Start>Shut Down>Shut Down**.
3. Turn on the workstation.
4. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

5. If you are using a a diskette, insert it now.
6. Select **File>Replicated Setup>Save to Removable Media**. Follow the instructions on the screen to create the configuration diskette.
7. Download a BIOS utility for replicating setup (repset.exe) and copy it onto the configuration diskette. To obtain this utility, go to http://welcome.hp.com/support/files and enter the model number of the workstation.
8. On the configuration diskette, create an autoexec.bat file containing the following command: **repset.exe**.
9. Turn off the workstation to be configured. Insert the configuration diskette and turn the workstation on. The configuration utility will run automatically.
10. Restart the workstation when the configuration is complete.

Dual-State Power Button

With Advanced Configuration and Power Interface (ACPI) enabled, the power button can function either as an on/off switch or as a standby button. The stand-by feature does not completely turn off power, but instead causes the workstation to enter a low-power standby state. This allows you to power down quickly without closing applications and to return quickly to the same operational state without any data loss.

To change the power button's configuration:

1 Click the **Start** button, then select **Control Panel>Power Options**.

2 In the **Power Options Properties**, select the **Advanced** tab.

3 In the **Power Button** section, select **Stand by**.

After configuring the power button to function as a standby button, press the power button to put the system in a very low power state (standby). Press the button again to quickly bring the system out of standby to full power status. To completely turn off all power to the system, press and hold the power button for four seconds.

CAUTION Do not use the power button to turn off the workstation unless the system is not responding; turning off the power without operating system interaction could cause damage to or loss of data on the hard drive.

World Wide Web Site

HP engineers rigorously test and debug software developed by HP and third-party suppliers, and develop operating system specific support software, to ensure performance, compatibility, and reliability for HP workstations.

When making the transition to new or revised operating systems, it is important to implement the support software designed for that operating system. If you plan to run a version of Microsoft Windows that is different from the version included with the workstation, you must install corresponding device drivers and utilities to ensure that all features are supported and functioning properly.

HP has made the task of locating, accessing, evaluating, and installing the latest support software easier. You can download the software from http://www.hp.com/support.

The Web site contains the latest device drivers, utilities, and flashable ROM images needed to run the latest Microsoft Windows operating system on the HP workstation.

Building Blocks and Partners

HP management solutions integrate with other systems management applications, and are based on industry standards, such as:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake on LAN Technology
- ACPI
- SMBIOS
- Pre-boot Execution (PXE) support

Asset Tracking and Security

Asset tracking features incorporated into the workstation provide key asset tracking data that can be managed using HP Systems Insight Manager, HP Client Manager Software or other system management applications. Seamless, automatic integration between asset tracking features and these products enables you to choose the management tool that is best suited to the environment and to leverage the investment in existing tools.

HP also offers several solutions for controlling access to valuable components and information. ProtectTools Embedded Security, if installed, prevents unauthorized access to data and checks system integrity and authenticates third-party users attempting system access. Security features such as ProtectTools, the Smart Cover Sensor and the Smart Cover Lock, available on select models, help to prevent unauthorized access to the internal components of the workstation. By disabling parallel, serial, or USB ports, or by disabling removable media boot capability, you can protect valuable data assets. Memory Change and Smart Cover Sensor alerts can be automatically forwarded to system management applications to deliver proactive notification of tampering with a workstation's internal components.

NOTE ProtectTools, the Smart Cover Sensor, and the Smart Cover Lock are available as options on select systems.

Use the following utilities to manage security settings on the HP workstation:

- Locally, using the Computer Setup Utilities.
- Remotely, using HP Client Manager Software or System Software Manager. This software enables the secure, consistent deployment and control of security settings from a simple command-line utility.

The following table and sections refer to managing security features of the workstation locally through the Computer Setup (F10) Utilities.

Table 3-3 Security Features Overview

Feature	Purpose	How it is Established
Removable Media Boot Control	Prevents booting from the removable media drives.	From the Setup Utilities menu.
Serial, Parallel, USB, or Infrared Interface Control	Prevents transfer of data through the integrated serial, parallel, USB, or infrared interface.	From the Setup Utilities menu.
Power-On Password	Prevents use of the workstation until the password is entered. This can apply to both initial system startup and restarts.	From the Setup Utilities menu.
Setup Password	Prevents reconfiguration of the workstation (use of the Setup Utilities) until the password is entered.	From the Setup Utilities menu.
Network Server Mode	Provides unique security features for workstations being used as servers.	From the Setup Utilities menu.
DriveLock	Prevents unauthorized access to the data on specific hard drives.	From the Setup Utilities menu.

Table 3-3 Security Features Overview

Feature	Purpose	How it is Established
Master Boot Record Security	Can prevent unintentional or malicious changes to the MBR of the current bootable disk and provides a means of recovering the “last known good” MBR.	From the Setup Utilities menu.
Ownership Tag	Displays ownership information, as defined by the system administrator, during system startup (protected by setup password).	From the Setup Utilities menu.
Cable Lock Provision	Prevents entire system theft only. 3mm x 7mm slot at rear of system.	Install a cable lock to secure the workstation to a fixed object, lock the access panel and secure internal components.
Padlock loop	Prevents access panel from being removed. This loop can also be used to secure the unit to a fixed object.	Install a padlock.
Solenoid Hood (Smart Cover) Lock (Optional)	Prevents removal of the access panel and all internal components including optical and diskette drives. Eliminates the need for a physical key by enabling password-protected locking & unlocking by a local or remote user. This feature is sold with the Hood Sensor.	Install a solenoid lock.
Hood Sensor (Optional)	Notifies a local or remote user when the chassis access panel has been opened. This feature is sold with the Solenoid Hood (Smart Cover) Lock.	Install an intrusion sensor.
Universal Chassis Clamp Lock (Optional)	The version without a cable discourages access panel removal and prevents theft of IO devices. The version with a cable additionally prevents entire system theft and allows multiple systems to be secured with a single cable.	Install a chassis clamp lock.
Rear Port Controller Cover	Clips to the back of the workstation and secures your input-output devices and prevents any cables at the back of the workstation from being removed.	Install a rear port controller cover.

NOTE: For more information about Computer Setup, see “Using Computer Setup (F10)” on page 36.

Password Security

The power-on password prevents unauthorized use of the workstation by requiring entry of a password to access applications or data each time the workstation is turned on or restarted. The setup password specifically prevents unauthorized access to Computer Setup, and can also be used as an override to the power-on password. That is, when prompted for the power-on password, entering the setup password instead will allow access to the workstation.

A network-wide setup password can be established to enable the system administrator to log in to all network systems to perform maintenance without having to know the power-on password.

NOTE System Software Manager and HP Client Manager Software allow remote management of Setup Passwords and other BIOS settings in a networked environment. For more information, visit http://www.hp.com/go/EasyDeploy.

ESTABLISHING A SETUP PASSWORD USING COMPUTER SETUP

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Embedded Security Guide*, on the *Documentation Library* CD. Establishing a setup password through Computer Setup prevents reconfiguration of the workstation (use of the Computer Setup (F10) utility) until the password is entered.

To establish a setup password using workstation setup:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. Select **Security>Setup Password** and follow the on-screen instructions.
4. Before exiting, select **File>Save Changes and Exit**.

ESTABLISHING A POWER-ON PASSWORD USING WORKSTATION SETUP

Establishing a power-on password through Computer Setup prevents access to the workstation when power is turned on, unless the password is entered. When a power-on password is set, Computer Setup presents Password Options under the Security menu. The password options include Network Server Mode and Password Prompt on Warm Boot.

When Network Server Mode is disabled, the password must be entered each time the workstation is turned on when the key icon appears on the monitor. When Password Prompt on Warm Boot is enabled, the password must also be entered each time the workstation is rebooted. When Network Server Mode is enabled, the password prompt is not presented during POST, but any attached PS/2 keyboard will remain locked until the user enters the power-on password.

To establish a power-on password through workstation setup:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. Select **Security>Power-On Password** and follow the on-screen instructions.
4. Before exiting, select **File>Save Changes and Exit**.

ENTERING A POWER-ON PASSWORD

To enter a power-on password:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart the Computer**.
2. When the key icon appears on the monitor, enter the current password, then press **Enter**.

NOTE Type carefully. For security reasons, the characters you enter do not appear on the screen.

If you enter the password incorrectly, a broken key icon appears. Try again. After three unsuccessful tries, you must turn off the workstation, then turn it on again before you can continue.

ENTERING A SETUP PASSWORD

If a setup password has been established on the workstation, you will be prompted to enter it each time you run Computer Setup.

To enter a setup password:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart the Computer**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. When the key icon appears on the monitor, enter the setup password, then press **Enter**.

NOTE Type carefully. For security reasons, the characters you enter do not appear on the screen.

If you enter the password incorrectly, a broken key icon appears. Try again. After three unsuccessful tries, you must turn off the workstation, then turn it on again before you can continue.

CHANGING A POWER-ON OR SETUP PASSWORD

To change a power-on or setup password:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart the Computer**. To change the setup password, run Computer Setup.
2. To change the Power-On password, go to step 3.

   To change the Setup password, wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. When the key icon appears, type the current password, a slash (/) or alternate delimiter character, your new password, another slash (/) or alternate delimiter character, and your new password again as shown:

   ```
   current password/new password/new password
   ```

NOTE Type carefully. For security reasons, the characters you enter do not appear on the screen.

4. Press **Enter**.

The new password takes effect the next time you turn on the workstation.

NOTE See the "National Keyboard Delimiter Characters" on page 58 for information about the alternate delimiter characters. The power-on password and setup password can also be changed using the Security options in Computer Setup.

Deleting a Power-On or Setup Password

To delete a power-on or setup password:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart the Computer**.
2. To delete the Power-On password, go to Step 3.

   To delete the Setup Password, wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the computer and try again to access the utility.

3. When the key icon appears, enter your current password followed by a slash (/) or alternate delimiter character as shown:

   ```
   current password/
   ```

4. Press **Enter**.

NOTE See the “National Keyboard Delimiter Characters” on page 58 section for information about the alternate delimiter characters. The power-on password and setup password can also be changed using the Security options in Computer Setup.

NATIONAL KEYBOARD DELIMITER CHARACTERS

Each keyboard is designed to meet country-specific requirements. The syntax and keys that you use for changing or deleting your password depend on the keyboard that came with your workstation.

Table 3-4 National Keyboard Delimiter Characters

Arabic	/	Greek	-	Russian	/
Belgian	=	Hebrew	.	Slovakian	-
BHCSY*	-	Hungarian	-	Spanish	-
Brazilian	/	Italian	-	Swedish/Finnish	/
Chinese	/	Japanese	/	Swiss	-
Czech	-	Korean	/	Taiwanese	/
Danish	-	Latin American	-	Thai	/
French	!	Norwegian	-	Turkish	.
French Canadian	é	Polish	-	U.K. English	/
German	-	Portuguese	-	U.S. English	/

*For Bosnia-Herzegovina, Croatia, Slovenia, and Yugoslavia

CLEARING PASSWORDS

If you forget your password, you cannot access the workstation. See Appendix H, “Additional Password Security and Resetting CMOS” for instructions on clearing passwords.

DriveLock

DriveLock prevents unauthorized access to the data on MultiBay hard drives. DriveLock has been implemented as an extension to Computer Setup. It is only available when DriveLock-capable hard drives are detected.

DriveLock employs a two-password security scheme. One password is intended to be set and used by a system administrator while the other is typically set and used by the end-user. There is no “back-door” that can be used to unlock the drive if both passwords are lost. Therefore, DriveLock is most safely used when the data contained on the hard drive is replicated on a corporate information system or is regularly backed-up.

CAUTION If both DriveLock passwords are lost, the hard drive is rendered unusable.

USING DRIVELOCK

The DriveLock option appears under the Security menu in Computer Setup. The user is presented with options to set the master password or to enable DriveLock. A user password must be provided to enable DriveLock. Since the initial configuration of DriveLock is typically performed by a system administrator, a master password should be set first. HP encourages system administrators to set a master password whether they plan to enable DriveLock or keep it disabled. This will give the administrator the ability to modify DriveLock settings if the drive is locked in the future. Once the master password is set, the system administrator can enable DriveLock or choose to keep it disabled.

If a locked hard drive is present, POST will require a password to unlock the device. If a power-on password is set and it matches the user password of the device, POST will not prompt the user to re-enter the password. Otherwise, the user will be prompted to enter a DriveLock password. Either the master or the user password can be used. Users will have two attempts to enter a correct password. If neither attempt succeeds, POST will continue but the data on the drive will remain inaccessible.

DRIVELOCK APPLICATIONS

The most practical use of the DriveLock security feature is in a corporate environment where a system administrator provides users with MultiBay hard drives for use in some desktop workstations. The system administrator would be responsible for configuring the MultiBay hard drive which would involve, among other things, setting the DriveLock master password. In the event that the user forgets the user password or the equipment is passed on to another employee, the master password can always be used to reset the user password and regain access to the hard drive.

HP recommends that corporate system administrators who choose to enable DriveLock also establish a corporate policy for setting and maintaining master passwords. This should be done to prevent a situation where an employee intentionally or unintentionally sets both DriveLock passwords before leaving the company. In such a scenario, the hard drive would be rendered unusable and require replacement. Likewise, by not setting a master password, system administrators might find themselves locked out of a hard drive and unable to perform routine checks for unauthorized software, other asset control functions and support.

For users with less stringent security requirements, HP does not recommend enabling DriveLock. Users in this category include personal users or users who do not maintain sensitive data on their hard drives as a common practice. For these users, the potential loss of a hard drive resulting from forgetting both passwords is much greater than the value of the data DriveLock has been designed to protect. Access to Computer Setup and DriveLock can be restricted through the Setup password. By specifying a Setup password and not giving it to end users, system administrators are able to restrict users from enabling DriveLock.

Hood Sensor

The hood sensor is an optional feature that is a combination of hardware and software technology that can alert you when the workstation access panel has been removed. This option is available as a kit that includes the solenoid hood (Smart Cover) lock (see the following section). There are three levels of protection, as described in the following table.

Table 3-5 Hood Sensor Protection Levels

Level	Setting	Description
Level 0	Disabled	Hood sensor is disabled (default).
Level 1	Notify User	When the workstation is restarted, the screen displays a message indicating that the workstation access panel has been removed.
Level 2	Setup Password	When the workstation is restarted, the screen displays a message indicating that the workstation access panel has been removed. You must enter the setup password to continue.
NOTE: These settings can be changed using Computer Setup.		

SETTING THE HOOD SENSOR PROTECTION LEVEL

To set the hood sensor protection level:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the computer and try again to access the utility.

3. Select **Security>Smart Cover>Cover Removal Sensor**, then access panel, and follow the on-screen instructions.
4. Before exiting, select **File>Save Changes and Exit**.

Solenoid Hood (Smart Cover) Lock

The solenoid hood lock is available as an option on HP Workstation xw4200 models (this option comes as a kit that includes the hood sensor). When installed, the solenoid hood lock can prevent unauthorized access to the internal components.

CAUTION For maximum cover lock security, be sure to establish a setup password. The setup password prevents unauthorized access to the Computer Setup utility.

LOCKING THE SOLENOID HOOD LOCK

To activate and lock the solenoid hood lock:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. Select **Security>Smart Cover>Cover Lock>Lock** option.
4. Before exiting, select **File>Save Changes and Exit**.

UNLOCKING THE SOLENOID HOOD LOCK

To unlock the solenoid hood lock:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. Select **Security>Smart Cover>Cover Lock>Unlock**.
4. Before exiting, select **File>Save Changes and Exit**.

USING THE ACCESS PANEL FAILSAFE KEY

If you enable the solenoid hood lock and cannot enter your password to disable the lock, you will need a access panel FailSafe Key to open the workstation access panel. You will need the key in any of the following circumstances:

- Power outage
- Startup failure
- PC component failure (such as processor or power supply)
- Forgotten password

CAUTION The access panel FailSafe Key is a specialized tool available from HP. Be prepared; order this key before you need one.

To obtain the FailSafe Key, complete any one of the following tasks:

- Contact your authorized HP reseller or service provider.
- Visit the HP Web site (http://www.hp.com) for ordering information.
- Visit the Contact HP Worldwide Web site (http://welcome.hp.com/country/us/en/wwcontact.html) for contact information.

Master Boot Record Security

The MBR contains information needed to successfully boot from a disk and to access the data stored on the disk. Master Boot Record Security detects and reports unintentional or malicious changes to the MBR, such as those caused by some workstation viruses or by the incorrect use of certain disk utilities. It also allows you to recover the “last known good” MBR, should changes to the MBR be detected when the system is restarted.

To enable MBR Security:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press the **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. Select **Security>Master Boot Record Security>Enabled**.
4. Select **Security>Save Master Boot Record**.
5. Before exiting, select **File>Save Changes and Exit**.

When MBR Security is enabled, the BIOS prevents any changes being made to the MBR of the current bootable disk while in MS-DOS or Windows Safe Mode.

NOTE Most operating systems control access to the MBR of the current bootable disk; the BIOS cannot prevent changes that might occur while the operating system is running.

Each time the workstation is turned on or restarted, the BIOS compares the MBR of the current bootable disk to the previously saved MBR. If changes are detected and if the current bootable disk is the same disk from which the MBR was previously saved, the following message is displayed:

```
1999 - Master Boot Record has changed.
Press any key to enter Setup to configure MBR Security.
```

Upon entering Computer Setup, you must perform one of the following tasks:

- Save the MBR of the current bootable disk
- Restore the previously saved MBR
- Disable the MBR Security feature

You must know the setup password, if one exists.

If changes are detected and if the current bootable disk is not the same disk from which the MBR was previously saved, the following message is displayed:

```
2000 - Master Boot Record Hard Drive has changed.
Press any key to enter Setup to configure MBR Security.
```

Upon entering Computer Setup, you must perform one of the following tasks:

- Save the MBR of the current bootable disk
- Disable the MBR Security feature

You must know the setup password, if one exists.

In the unlikely event that the previously saved MBR has been corrupted, the following message is displayed:

```
1998 - Master Boot Record has been lost.
Press any key to enter Setup to configure MBR Security.
```

Upon entering Computer Setup, you must perform one of the following tasks:

- Save the MBR of the current bootable disk
- Disable the MBR Security feature

You must know the setup password, if one exists.

Before You Partition or Format the Current Bootable Disk

Before you partition or format the current bootable disk, ensure that MBR Security is disabled before you change partitioning or formatting of the current bootable disk. Some disk utilities, such as FDISK and FORMAT, attempt to update the MBR. If MBR Security is enabled when you change partitioning or formatting of the disk, you might receive error messages from the disk utility or a warning from MBR Security the next time the workstation is turned on or restarted.

To disable MBR Security:

1. Turn on or restart the workstation. If you are in Windows, click **Start>Shut Down>Restart the Computer**.
2. Wait for the `F10=Setup` prompt to appear on the lower right corner of the screen. Once you see the prompt, press the **F10** key to enter the F10 setup utility.

NOTE If you do not press **F10** key at the appropriate time, you must restart the workstation and try again to access the utility.

3. Select **Security>Master Boot Record Security>Disabled**.
4. Before exiting, select **File>Save Changes and Exit**.

Cable Lock Slot

The rear panel of the chassis can accommodate a cable lock accessory that allows the workstation to be physically secured to a work area.

For illustrated instructions, see “Cable Lock (Optional)” on page 75.

Padlock (Optional)

Prevents entire system theft and discourages access panel removal.

For illustrated instructions, see “Security Padlock (Optional)” on page 75.

Universal Chassis Clamp Lock (Optional)

The version without a cable discourages access panel removal and prevents theft of IO devices. The version with a cable also prevents entire system theft and allows multiple systems to be secured with a single cable.

For illustrated instructions, see “Universal Chassis Clamp Lock (Optional)” on page 76.

Rear Port Controller Cover (Optional)

Locks rear I/O cables to prevent cable theft.

Fingerprint Identification Technology

Eliminating the need to enter user passwords, HP Fingerprint Identification Technology tightens network security, simplifies the login process, and reduces the costs associated with managing corporate networks. Affordably priced, it is not just for high-tech, high-security organizations anymore.

Support for Fingerprint Identification Technology varies by model.

For more information, visit http://ht8004.www1,hp.com/products/security.

Fault Notification and Recovery

Fault Notification and Recovery features combine innovative hardware and software technology to prevent the loss of critical data and minimize unplanned downtime.

If the workstation is connected to a network managed by HP Client Manager Software, the computer sends a fault notice to the network management application. With HP Client Manager Software, you can also remotely schedule diagnostics to automatically run on all managed PCs and create a summary report of failed tests.

Drive Protection System

The DPS is a diagnostic tool built into the hard drives installed in select HP workstations. DPS is designed to help diagnose problems that might result in unwarranted hard drive replacement.

When HP workstations are built, each installed hard drive is tested using DPS, and a permanent record of key information is written onto the drive. Each time DPS is run, test results are write to the hard drive. Each time DPS is run, test results are written to the hard drive. The service provider can use this information to help diagnose conditions that caused you to run the DPS software.

Ultra ATA Integrity Monitoring

Ultra ATA Integrity Monitoring monitors the integrity of data as it is transferred between an Ultra ATA hard drive and the system's core logic. If the workstation detects an abnormal number of transmission errors, the workstation displays a Local Alert message with recommended actions.

ECC Fault Prediction and Prefailure Warranty

When the workstation encounters an excessive number of error checking and correcting (ECC) memory errors, the workstation displays a Local Alert message. This message contains detailed information about the errant memory module, allowing you to take action before you experience non-correctable memory errors. The Prefailure Warranty for ECC memory modules allows you to replace these modules, free of charge, before the modules actually fail. ECC memory modules are optional on selected HP systems.

NOTE To use this feature, you must replace the standard DIMMs with HP ECC DIMMs.

Surge-Tolerant Power Supply

An integrated surge-tolerant power supply provides greater reliability when the workstation is hit with an unpredictable power surge. This power supply is rated to withstand a power surge of up to 2000 V (Line to PE or Neutral to PE) and 1000 V (Line to Line) without any data loss or system downtime.

Thermal Sensor

The thermal sensor is a hardware and software feature that tracks the internal temperature of the workstation. When combined with HP Client Manager Software, this feature notifies the network administrator when the normal range is exceeded.

The thermal sensor monitors the processor temperature and if the temperature gets too hot, the processor clock automatically begins to throttle. If the temperature does not go down, then the system eventually shuts down.